

We claim:

1 1. A system for providing continuous authentication of a user of a computing device,

2 comprising:

3 a security component which provides security functions, such that the security component
4 can vouch for authenticity of one or more other components with which it is securely operably
5 connected;

6 a biometric sensor component that is securely operably connected, as one of the one or
7 more other components, to the security component;

8 securely-stored biometric information which identifies an owner of the computing device;
9 means for repeatedly obtaining, from the biometric sensor component, biometric input of a
10 user of the computing device; and

11 means for comparing the repeatedly obtained biometric input to the securely-stored
12 biometric information of the owner, wherein each of the comparisons comprises an authentication
13 of the user.

1 2. The system according to Claim 1, wherein the means for repeatedly obtaining is activated
2 upon beginning a security-sensitive operation and is terminated upon completion of the security-
3 sensitive operation.

1 3. The system according to Claim 1, wherein the means for repeatedly obtaining is activated
2 each time a predetermined time interval elapses.

1 4. The system according to Claim 3, wherein the predetermined time interval is selectively
2 configured by the owner of the computing device.

1 5. The system according to Claim 1, wherein the means for repeatedly obtaining is activated
2 upon switching between functions of the computing device.

1 6. The system according to Claim 1, wherein the means for repeatedly obtaining is activated
2 upon switching between functions of an application that is executing a security-sensitive operation
3 using the computing device.

1 7. The system according to Claim 1, wherein the means for repeatedly obtaining is activated
2 when the biometric sensor component detects one or more of an interruption, change, or loss of
3 the biometric input.

1 8. The system according to Claim 1, wherein the means for repeatedly obtaining is activated
2 upon reaching one of at least one predetermined instructions in an application that is executing a
3 security-sensitive operation using the computing device.

1 9. The system according to Claim 1, wherein the biometric sensor component is securely
2 operably connected to the security component when the security component is manufactured.

13. The system according to Claim 1, wherein the means for securely operably connecting is
2 activated by a hardware reset of the biometric sensor component, and wherein the hardware reset
3 is activated by operably connecting of the biometric sensor component.

14. The system according to Claim 11, wherein the means for authenticating the biometric
2 sensor component is securely stored thereon.

1 15. The system according to Claim 11, wherein the means for authenticating further comprises
2 means for using public key cryptography.

1 17. The system according to Claim 1, wherein the biometric sensor component is a fingerprint
2 sensor, and wherein the fingerprint sensor is capable of repeatedly obtaining a fingerprint of the
3 user as the biometric input of the user while the computing device is being held by the user.

1 18. The system according to Claim 1, wherein the biometric sensor component is a retina
2 scanner, and wherein the retina scanner is capable of repeatedly obtaining a retinal scan of the user
3 as the biometric input of the user while the user is looking at the computing device.

1 19. The system according to Claim 1, wherein the means for comparing is performed by the
2 biometric sensor component.

1 20. The system according to Claim 19, further comprising means for securely transferring the
2 securely-stored biometric information of the owner to the biometric sensor component for use by
3 the means for comparing.

1 21. The system according to Claim 1, wherein the means for comparing is performed by the
2 security component.

1 22. The system according to Claim 2, further comprising means for aborting the security-
2 sensitive operation if the means for repeatedly obtaining or the means for comparing fails to detect

3 the biometric information of the user, thereby causing the completion of the security-sensitive
4 operation.

1 23. The system according to Claim 2, further comprising means for marking the security-
2 sensitive operation as not authenticated if the means for repeatedly obtaining or the means for
3 comparing fails to detect the biometric information of the user.

1 24. The system according to Claim 2, further comprising means for deactivating the
2 computing device if the means for repeatedly obtaining or the means for comparing fails to detect
3 the biometric information of the user.

1 25. The system according to Claim 2, further comprising means for concluding that the
2 security-sensitive operation is authentic if the means for comparing succeeds until completion of
3 the security-sensitive operation.

1 26. The system according to Claim 25, wherein the means for concluding that the security-
2 sensitive operation is authentic also requires that all other components which are securely
3 operably connected to the security core remain securely operably connected until completion of
4 the security-sensitive operation.

1 27. The system according to Claim 25, wherein the means for concluding that the security-
2 sensitive operation is authentic also requires that all other components which are securely

3 operably connected to the security core and which are involved in the security-sensitive operation
4 remain securely operably connected until completion thereof.

1 28. The system according to Claim 11, wherein the means for authenticating further comprises
2 means for performing a security handshake between the biometric sensor component and the
3 security component.

1 29. The system according to Claim 11, wherein the biometric sensor component has
2 associated therewith a unique device identifier that is used to identify data originating therefrom, a
3 digital certificate, a private cryptographic key and a public cryptographic key that is
4 cryptographically-associated with the private cryptographic key.

1 30. The system according to Claim 1, wherein the biometric sensor component is physically
2 integrated with a card, and wherein a card reader adapted to reading the card is securely operably
3 connected to the security component.

1 31. The system according to Claim 1 or Claim 30, further comprising:
2 previously-stored secrets of the owner of the computing device; and
3 means for accessing selected ones of the previously-stored secrets only if the means for
4 comparing determines, over a duration of a security-sensitive operation, that the obtained
5 biometric input of the user matches the securely-stored biometric information of the owner.

1 32. The system according to Claim 31, wherein the previously-stored secrets include a private
2 cryptographic key of the owner, and wherein the means for accessing further comprises means for
3 accessing the private key to compute a digital signature over information pertaining to the
4 security-sensitive operation.

1 33. The system according to Claim 1, wherein the means for repeatedly obtaining is activated
2 continually during an interval of a security-sensitive operation being performed with the
3 computing device.

1 34. The system according to Claim 11, wherein the means for authenticating further comprises
2 means for using (1) a unique identifier of the biometric sensor component, (2) a digital signature
3 computed over the unique identifier using a private cryptographic key of the biometric sensor
4 component, and (3) a public key that is cryptographically associated with the private key.

1 35. A method for providing continuous authentication of a user of a computing device,
2 comprising steps of:

3 operating a security component which provides security functions, such that the security
4 component can vouch for authenticity of one or more other components with which it is securely
5 operably connected;

6 providing a biometric sensor component that is securely operably connected, as one of the
7 one or more other components, to the security component;

8 providing securely-stored biometric information which identifies an owner of the
9 computing device;
10 repeatedly obtaining, from the biometric sensor component, biometric input of a user of
11 the computing device; and
12 comparing the repeatedly obtained biometric input to the securely-stored biometric
13 information of the owner, wherein each of the comparisons comprises an authentication of the
14 user.

1 36. The method according to Claim 35, wherein the step of repeatedly obtaining is activated
2 upon beginning a security-sensitive operation and is terminated upon completion of the security-
3 sensitive operation.

1 37. The method according to Claim 35, wherein the step of repeatedly obtaining is activated
2 each time a predetermined time interval elapses.

1 38. The method according to Claim 37, wherein the predetermined time interval is selectively
2 configured by the owner of the computing device.

1 39. The method according to Claim 35, wherein the step of repeatedly obtaining is activated
2 upon switching between functions of the computing device.

1 40. The method according to Claim 35, wherein the step of repeatedly obtaining is activated
2 upon switching between functions of an application that is executing a security-sensitive operation
3 using the computing device.

1 41. The method according to Claim 35, wherein the step of repeatedly obtaining is activated
2 when the biometric sensor component detects one or more of an interruption, change, or loss of
3 the biometric input.

1 42. The method according to Claim 35, wherein the step of repeatedly obtaining is activated
2 upon reaching one of at least one predetermined instructions in an application that is executing a
3 security-sensitive operation using the computing device.

1 43. The method according to Claim 35, wherein the biometric sensor component is securely
2 operably connected to the security component when the security component is manufactured.

1 44. The method according to Claim 35, wherein the other components comprise one or more
2 of (1) input/output components and (2) application processing components.

1 45. The method according to Claim 35, wherein the step of securely operably connecting
2 further comprises the step of authenticating the biometric sensor component to the security
3 component.

1 46. The method according to Claim 45, further comprising the step of authenticating the
2 security component to the biometric sensor component.

1 47. The method according to Claim 35, wherein the step of securely operably connecting is
2 activated by a hardware reset of the biometric sensor component, and wherein the hardware reset
3 is activated by operably connecting of the biometric sensor component.

1 48. The method according to Claim 45, wherein instructions to perform the step of
2 authenticating the biometric sensor component are securely stored thereon.

1 49. The method according to Claim 45, wherein the step of authenticating further comprises
2 the step of using public key cryptography.

1 50. The method according to Claim 35, further comprising the step of concluding that the user
2 is the owner of the computing device only if the comparing step succeeds.

1 51. The method according to Claim 35, wherein the biometric sensor component is a
2 fingerprint sensor, and wherein the fingerprint sensor is capable of repeatedly obtaining a
3 fingerprint of the user as the biometric input of the user while the computing device is being held
4 by the user.

1 52. The method according to Claim 35, wherein the biometric sensor component is a retina
2 scanner, and wherein the retina scanner is capable of repeatedly obtaining a retinal scan of the user
3 as the biometric input of the user while the user is looking at the computing device.

1 53. The method according to Claim 35, wherein the comparing step is performed by the
2 biometric sensor component.

1 54. The method according to Claim 53, further comprising the step of securely transferring the
2 securely-stored biometric information of the owner to the biometric sensor component for use by
3 the comparing step.

1 55. The method according to Claim 35, wherein the comparing step is performed by the
2 security component.

1 56. The method according to Claim 36, further comprising the step of aborting the security-
2 sensitive operation if the step of repeatedly obtaining or the comparing step fails to detect the
3 biometric information of the user, thereby causing the completion of the security-sensitive
4 operation.

1 57. The method according to Claim 36, further comprising the step of marking the security-
2 sensitive operation as not authenticated if the step of repeatedly obtaining or the comparing step
3 fails to detect the biometric information of the user.

1 59. The method according to Claim 36, further comprising the step of concluding that the
2 security-sensitive operation is authentic if the comparing step succeeds until completion of the
3 security-sensitive operation.

1 60. The method according to Claim 59, wherein the step of concluding that the security-
2 sensitive operation is authentic also requires that all other components which are securely
3 operably connected to the security core remain securely operably connected until completion of
4 the security-sensitive operation.

61. The method according to Claim 59, wherein the step of concluding that the security-
2 sensitive operation is authentic also requires that all other components which are securely
3 operably connected to the security core and which are involved in the security-sensitive operation
4 remain securely operably connected until completion thereof.

1 62. The method according to Claim 45, wherein the step of authenticating further comprises
2 the step of performing a security handshake between the biometric sensor component and the
3 security component.

1 63. The method according to Claim 45, wherein the biometric sensor component has
2 associated therewith a unique device identifier that is used to identify data originating therefrom, a
3 digital certificate, a private cryptographic key and a public cryptographic key that is
4 cryptographically-associated with the private cryptographic key.

1 64. The method according to Claim 35, wherein the biometric sensor component is physically
2 integrated with a card, and wherein a card reader adapted to reading the card is securely operably
3 connected to the security component.

1 65. The method according to Claim 35, further comprising steps of:
2 providing previously-stored secrets of the owner of the computing device; and
3 accessing selected ones of the previously-stored secrets only if the comparing step
4 determines, over a duration of a security-sensitive operation, that the obtained biometric input of
the user matches the securely-stored biometric information of the owner.

1 66. The method according to Claim 65, wherein the previously-stored secrets include a private
2 cryptographic key of the owner, and wherein the accessing step further comprises the step of
3 accessing the private key to compute a digital signature over information pertaining to the
4 security-sensitive operation.

1 67. The method according to Claim 35, wherein the step of repeatedly obtaining is activated
2 continually during an interval of a security-sensitive operation being performed with the
3 computing device.

1 68. The method according to Claim 45, wherein the step of authenticating further comprises
2 the step of using (1) a unique identifier of the biometric sensor component, (2) a digital signature
3 computed over the unique identifier using a private cryptographic key of the biometric sensor
4 component, and (3) a public key that is cryptographically associated with the private key.

1 69. A computer program product for providing continuous authentication of a user of a
2 computing device, the computer program product embodied on one or more computer-readable
3 media and comprising:

4 computer-readable program code means for operating a security component which
5 provides security functions, such that the security component can vouch for authenticity of one or
6 more other components with which it is securely operably connected;

7 computer-readable program code means for accessing a biometric sensor component that
8 is securely operably connected, as one of the one or more other components, to the security
9 component;

10 computer-readable program code means for accessing securely-stored biometric
11 information which identifies an owner of the computing device;

12 computer-readable program code means for repeatedly obtaining, from the biometric
13 sensor component, biometric input of a user of the computing device; and

14 computer-readable program code means for comparing the repeatedly obtained biometric
15 input to the securely-stored biometric information of the owner, wherein each of the comparisons
16 comprises an authentication of the user.

1 70. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for repeatedly obtaining is activated upon beginning a security-sensitive
3 operation and is terminated upon completion of the security-sensitive operation.

1 71. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for repeatedly obtaining is activated each time a predetermined time interval
3 elapses.

1 72. The computer program product according to Claim 71, wherein the predetermined time
2 interval is selectively configured by the owner of the computing device.

1 73. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for repeatedly obtaining is activated upon switching between functions of
3 the computing device.

1 74. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for repeatedly obtaining is activated upon switching between functions of an
3 application that is executing a security-sensitive operation using the computing device.

1 75. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for repeatedly obtaining is activated when the biometric sensor component
3 detects one or more of an interruption, change, or loss of the biometric input.

1 76. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for repeatedly obtaining is activated upon reaching one of at least one
3 predetermined instructions in an application that is executing a security-sensitive operation using
4 the computing device.

1 77. The computer program product according to Claim 69, wherein the biometric sensor
2 component is securely operably connected to the security component when the security
3 component is manufactured.

1 78. The computer program product according to Claim 69, wherein the other components
2 comprise one or more of (1) input/output components and (2) application processing components.

1 79. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for securely operably connecting further comprises computer-readable
3 program code means for authenticating the biometric sensor component to the security
4 component.

1 80. The computer program product according to Claim 79, further comprising computer-
2 readable program code means for authenticating the security component to the biometric sensor
3 component.

1 81. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for securely operably connecting is activated by a hardware reset of the
3 biometric sensor component, and wherein the hardware reset is activated by operably connecting
4 of the biometric sensor component.

1 82. The computer program product according to Claim 79, wherein the computer-readable
2 program code means for authenticating the biometric sensor component is securely stored
3 thereon.

1 83. The computer program product according to Claim 79, wherein the computer-readable
2 program code means for authenticating further comprises computer-readable program code means
3 for using public key cryptography.

1 84. The computer program product according to Claim 69, further comprising computer-
2 readable program code means for concluding that the user is the owner of the computing device
3 only if the computer-readable program code means for comparing succeeds.

1 85. The computer program product according to Claim 69, wherein the biometric sensor
2 component is a fingerprint sensor, and wherein the fingerprint sensor is capable of repeatedly
3 obtaining a fingerprint of the user as the biometric input of the user while the computing device is
4 being held by the user.

1 86. The computer program product according to Claim 69, wherein the biometric sensor
2 component is a retina scanner, and wherein the retina scanner is capable of repeatedly obtaining a
3 retinal scan of the user as the biometric input of the user while the user is looking at the
4 computing device.

1 87. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for comparing is performed by the biometric sensor component.

1 88. The computer program product according to Claim 87, further comprising computer-
2 readable program code means for securely transferring the securely-stored biometric information
3 of the owner to the biometric sensor component for use by the computer-readable program code
4 means for comparing.

1 89. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for comparing is performed by the security component.

1 90. The computer program product according to Claim 70, further comprising computer-
2 readable program code means for aborting the security-sensitive operation if the computer-
3 readable program code means for repeatedly obtaining or the computer-readable program code
4 means for comparing fails to detect the biometric information of the user, thereby causing the
5 completion of the security-sensitive operation.

1 91. The computer program product according to Claim 70, further comprising computer-
2 readable program code means for marking the security-sensitive operation as not authenticated if
3 the computer-readable program code means for repeatedly obtaining or the computer-readable
4 program code means for comparing fails to detect the biometric information of the user.

1 92. The computer program product according to Claim 70, further comprising computer-
2 readable program code means for deactivating the computing device if the computer-readable
3 program code means for repeatedly obtaining or the computer-readable program code means for
4 comparing fails to detect the biometric information of the user.

1 93. The computer program product according to Claim 70, further comprising computer-
2 readable program code means for concluding that the security-sensitive operation is authentic if
3 the computer-readable program code means for comparing succeeds until completion of the
4 security-sensitive operation.

1 94. The computer program product according to Claim 93, wherein the computer-readable
2 program code means for concluding that the security-sensitive operation is authentic also requires
3 that all other components which are securely operably connected to the security core remain
4 securely operably connected until completion of the security-sensitive operation.

1 95. The computer program product according to Claim 93, wherein the computer-readable
2 program code means for concluding that the security-sensitive operation is authentic also requires
3 that all other components which are securely operably connected to the security core and which
4 are involved in the security-sensitive operation remain securely operably connected until
completion thereof.

1 96. The computer program product according to Claim 79, wherein the computer-readable
2 program code means for authenticating further comprises computer-readable program code means
3 for performing a security handshake between the biometric sensor component and the security
component.

1 97. The computer program product according to Claim 79, wherein the biometric sensor
2 component has associated therewith a unique device identifier that is used to identify data
3 originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic
4 key that is cryptographically-associated with the private cryptographic key.

1 98. The computer program product according to Claim 69, wherein the biometric sensor
2 component is physically integrated with a card, and wherein a card reader adapted to reading the
3 card is securely operably connected to the security component.

1 99. The computer program product according to Claim 98, further comprising:
2 computer-readable program code means for accessing previously-stored secrets of the
3 owner of the computing device; and
4 computer-readable program code means for accessing selected ones of the previously-
5 stored secrets only if the computer-readable program code means for comparing determines, over
6 a duration of a security-sensitive operation, that the obtained biometric input of the user matches
7 the securely-stored biometric information of the owner.

1 100. The computer program product according to Claim 99, wherein the previously-stored
2 secrets include a private cryptographic key of the owner, and wherein the computer-readable
3 program code means for accessing further comprises computer-readable program code means for
4 accessing the private key to compute a digital signature over information pertaining to the
5 security-sensitive operation.

1 101. The computer program product according to Claim 69, wherein the computer-readable
2 program code means for repeatedly obtaining is activated continually during an interval of a
3 security-sensitive operation being performed with the computing device.

1 102. The computer program product according to Claim 79, wherein the computer-readable
2 program code means for authenticating further comprises computer-readable program code means
3 for using (1) a unique identifier of the biometric sensor component, (2) a digital signature
4 computed over the unique identifier using a private cryptographic key of the biometric sensor
5 component, and (3) a public key that is cryptographically associated with the private key.

1 103. A method of doing business by continually authenticating a user of a computing device,
2 comprising steps of:

3 operating a security component for the computing device, wherein the security component
4 provides security functions such that the security component can vouch for authenticity of one or
5 more other components with which it is securely operably connected;

6 providing a biometric sensor component that is securely operably connected, as one of the
7 one or more other components, to the security component;

8 providing securely-stored biometric information which identifies an owner of the
9 computing device;

10 performing a security-sensitive operation using the computing device;

11 repeatedly obtaining, from the biometric sensor component, biometric input of a user of
12 the computing device over a duration of the security-sensitive operation;

13 comparing the repeatedly obtained biometric input to the securely-stored biometric
14 information of the owner, wherein each of the comparisons comprises an authentication of the
15 user; and

16 aborting the security-sensitive operation if the comparing step fails at any time over the
17 duration of the security-sensitive operation.

1 104. A method of improving security of a computing device, comprising steps of:
2 operating a security component for the computing device, wherein the security component
3 provides security functions such that the security component can vouch for authenticity of one or
4 more other components with which it is securely operably connected;
5 providing a biometric sensor component that is securely operably connected, as one of the
6 one or more other components, to the security component;
7 providing securely-stored biometric information which identifies an owner of the
8 computing device;
9 repeatedly obtaining, from the biometric sensor component, biometric input of a user of
10 the computing device; and
11 comparing the repeatedly obtained biometric input to the securely-stored biometric
12 information of the owner.

1 105. A method of improving security of operations carried out with a computing device,
2 comprising steps of:
3 operating a security component for the computing device, wherein the security component
4 provides security functions such that the security component can vouch for authenticity of one or
5 more other components with which it is securely operably connected;

6 providing a biometric sensor component that is securely operably connected, as one of the
7 one or more other components, to the security component;

8 providing securely-stored biometric information which identifies an owner of the
9 computing device;

10 performing a security-sensitive operation using the computing device;

11 repeatedly obtaining, from the biometric sensor component, biometric input of a user of
12 the computing device over a duration of the security-sensitive operation;

13 comparing the repeatedly obtained biometric input to the securely-stored biometric
14 information of the owner, wherein each of the comparisons comprises an authentication of the
15 user; and

16 aborting the security-sensitive operation if the comparing step fails at any time over the
17 duration of the security-sensitive operation.